PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-141916
(43)Date of publication of application : 17.05.2002

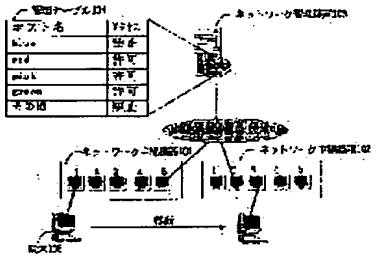
(51)Int.Cl. H04L 12/28
H04L 12/44

(21)Application number : 2000-337266
(22)Date of filing : 31.10.2000

(71)Applicant : HITACHI CABLE LTD
(72)Inventor : HIRAOKA DAIKI

(54) NETWORK MANAGEMENT SYSTEM, AND NETWORK REPEATER AND NETWORK MANAGEMENT DEVICE USED FOR THE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a network management system ensuring the security, and a network repeater and a network management device used for the system.
SOLUTION: The network repeater 101 transmits information of a terminal 105 connected to the repeater 101 to the network management device 103, which returns information denoting an access permission/inhibition to the network repeater 101 depending on the terminal information, and the network repeater 101 sets use permission/use inhibit to a port to which the terminal 105 is connected based on the access permission/inhibition information. Since the permission/inhibition of the port to which the terminal 105 is connected is set depending on the terminal information managed by the network management device 103, the security is ensured without disturbing the use of a legal terminal.



LEGAL STATUS

[Date of request for examination] 18.11.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－141916
（Ｐ２００２－１４１９１６Ａ）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
H04L 12/28		H04L 11/00	310	D 5K033
12/44			340	

審査請求　未請求　請求項の数23　ＯＬ　（全10頁）

(21)出願番号　特願2000－337266（Ｐ2000－337266）

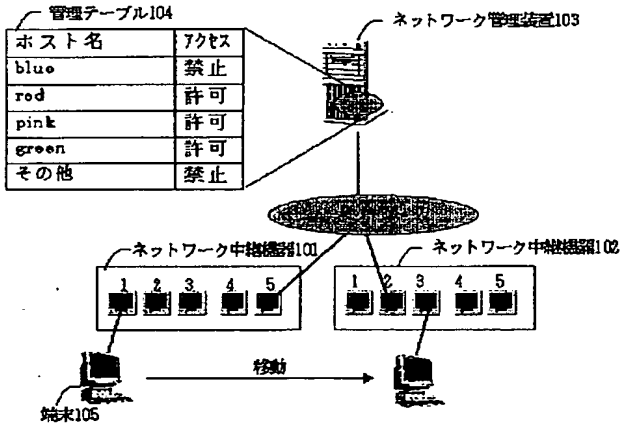
(22)出願日　平成12年10月31日(2000.10.31)

(71)出願人　000005120
日立電線株式会社
東京都千代田区大手町一丁目６番１号
(72)発明者　平岡　大樹
茨城県日立市砂沢町880番地　日立電線株式会社高砂工場内
(74)代理人　100068021
弁理士　絹谷　信雄

Ｆターム(参考)　5K033 BA04 BA08 DA05 DA15 DB12 DB14 DB17 DB18 DB20 EA07 EC01

(54)【発明の名称】ネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置

(57)【要約】
【課題】　セキュリティを確保できるネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置を提供する。
【解決手段】　ネットワーク中継機器１０１より接続されている端末１０５の情報をネットワーク管理装置１０３に送信し、そのネットワーク管理装置１０３が前記端末情報に応じてアクセス許可／禁止を示す情報をネットワーク中継機器１０１に返信し、ネットワーク中継機器１０１が前記アクセス許可／禁止情報に基づいて端末１０５を接続しているポートを使用可能／使用不可に設定する。ネットワーク管理装置１０３が管理する端末情報に応じてネットワーク中継機器１０１のポートの使用可否が設定されるので、正当な端末の利用を妨げることなくセキュリティが確保される。



1

【特許請求の範囲】

【請求項１】　ネットワーク中継機器より接続されている端末の情報をネットワーク管理装置に送信し、そのネットワーク管理装置が前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信し、前記ネットワーク中継機器が前記アクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定することを特徴とするネットワーク管理システム。

【請求項２】　前記端末情報は、当該端末を使用しているユーザの識別情報であることを特徴とする請求項１記載のネットワーク管理システム。

【請求項３】　前記端末情報は、当該端末のホスト名であることを特徴とする請求項１記載のネットワーク管理システム。

【請求項４】　前記端末情報は、当該端末のＩＰアドレスであることを特徴とする請求項１記載のネットワーク管理システム。

【請求項５】　前記端末情報は、当該端末のＭＡＣアドレスであることを特徴とする請求項１記載のネットワーク管理システム。

【請求項６】　ネットワーク中継機器において、接続されている端末の情報をネットワーク管理装置に送信する機能を備えたことを特徴とするネットワーク中継機器。

【請求項７】　前記端末情報の送信に対する返信として前記ネットワーク管理装置からアクセス許可／禁止を示す情報を受信した場合、このアクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定する機能を備えたことを特徴とする請求項６記載のネットワーク中継機器。

【請求項８】　前記端末情報をネットワーク管理装置に送信するポートと前記端末情報をネットワーク管理装置に送信しないポートとの設定がポート毎にできる機能を備えたことを特徴とする請求項６又は７記載のネットワーク中継機器。

【請求項９】　前記端末情報をネットワーク管理装置に送信しないポートに対し任意にポートの使用可否が設定できる機能を備えたことを特徴とする請求項８記載のネットワーク中継機器。

【請求項１０】　前記端末情報をどのネットワーク管理装置に送信するかを指定しておくことができる機能を備えたことを特徴とする請求項６～９いずれか記載のネットワーク中継機器。

【請求項１１】　前記端末情報の送信に対する前記ネットワーク管理装置からの返信がなかった場合、端末が接続されているポートの使用可否が予め設定できる機能を備えたことを特徴とする請求項６～１０いずれか記載のネットワーク中継機器。

【請求項１２】　前記端末情報は、当該端末が送信するデータの内容から取得した当該端末を使用しているユーザの識別情報であることを特徴とする請求項６～１１いずれか記載のネットワーク中継機器。

2

【請求項１３】　前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のホスト名であることを特徴とする請求項６～１１のいずれか記載のネットワーク中継機器。

【請求項１４】　前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のＩＰアドレスであることを特徴とする請求項６～１１いずれか記載のネットワーク中継機器。

【請求項１５】　前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のＭＡＣアドレスであることを特徴とする請求項６～１１いずれか記載のネットワーク中継機器。

【請求項１６】　ネットワーク管理装置において、ネットワーク中継機器から端末の情報を受信した場合、前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信する機能を備えたことを特徴とするネットワーク管理装置。

【請求項１７】　前記ネットワーク中継機器に返信するべきアクセス許可／禁止を示す情報と前記端末情報との対応を管理できる機能を備えたことを特徴とする請求項１６記載のネットワーク管理装置。

【請求項１８】　前記端末情報は、当該端末を使用しているユーザの識別情報であることを特徴とする請求項１６又は１７記載のネットワーク管理装置。

【請求項１９】　前記端末情報は、当該端末のホスト名であることを特徴とする請求項１６又は１７記載のネットワーク管理装置。

【請求項２０】　前記端末情報は、当該端末のＩＰアドレスであることを特徴とする請求項１６又は１７記載のネットワーク管理装置。

【請求項２１】　前記端末情報は、当該端末のＭＡＣアドレスであることを特徴とする請求項１６又は１７記載のネットワーク管理装置。

【請求項２２】　ＩＰアドレスと有効ビットマスク値とを組として複数のＩＰアドレスを指定するＩＰサブネットを用い、このＩＰサブネットとアクセス許可／禁止情報との対応を定義しておき、この定義に照らして前記アクセス許可／禁止情報と前記端末のＩＰアドレスとの対応を管理する機能を備えたことを特徴とする請求項２０記載のネットワーク管理装置。

【請求項２３】　前記ネットワーク中継機器からの送信及びその送信に対する返信の内容をログとして記録し、このログを管理画面から参照できる機能を備えたことを特徴とする請求項１６～２２いずれか記載のネットワーク管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワーク中継

機器を用いたネットワーク管理システムに係り、特に、セキュリティを確保できるネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置に関するものである。

【０００２】

【従来の技術】多くのネットワーク中継機器は、ポートの使用可否の設定機能を備えている。ポートを使用不可に設定すると、そのポートに接続されたネットワーク機器は前記ネットワーク中継機器を介して通信を行うことができない。

【０００３】

【発明が解決しようとする課題】ネットワーク上に設置されているネットワーク中継機器に、どの端末を接続しても、ポートが使用可能に設定されていれば、その端末は前記ネットワーク中継機器を介して通信を行うことができる。仮に、悪意を持った外部からの侵入者の端末でも同様に通信を行うことができる。侵入者の端末がネットワークにアクセスできないようポートを使用不可に設定すると、本来、ネットワークにアクセスが許されるべき端末をもネットワークにアクセスさせないことになってしまう。このように、従来のネットワーク中継機器を用いたネットワーク管理システムではセキュリティの確保が難しい。

【０００４】そこで、本発明の目的は、上記課題を解決し、セキュリティを確保できるネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置を提供することにある。

【０００５】

【課題を解決するための手段】上記目的を達成するために本発明のネットワーク管理装置は、ネットワーク中継機器より接続されている端末の情報をネットワーク管理装置に送信し、そのネットワーク管理装置が前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信し、前記ネットワーク中継機器が前記アクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定するものである。

【０００６】前記端末情報は、当該端末を使用しているユーザの識別情報であってもよい。

【０００７】前記端末情報は、当該端末のホスト名であってもよい。

【０００８】前記端末情報は、当該端末のＩＰアドレスであってもよい。

【０００９】前記端末情報は、当該端末のＭＡＣアドレスであってもよい。

【００１０】また、本発明のネットワーク中継機器は、接続されている端末の情報をネットワーク管理装置に送信する機能を備えたものである。

【００１１】前記端末情報の送信に対する返信として前記ネットワーク管理装置からアクセス許可／禁止を示す情報を受信した場合、このアクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定する機能を備えてもよい。

【００１２】前記端末情報をネットワーク管理装置に送信するポートと前記端末情報をネットワーク管理装置に送信しないポートとの設定がポート毎にできる機能を備えてもよい。

【００１３】前記端末情報をネットワーク管理装置に送信しないポートに対し任意にポートの使用可否が設定できる機能を備えてもよい。

【００１４】前記端末情報をどのネットワーク管理装置に送信するかを指定しておくことができる機能を備えてもよい。

【００１５】前記端末情報の送信に対する前記ネットワーク管理装置からの返信がなかった場合、端末が接続されているポートの使用可否が予め設定できる機能を備えてもよい。

【００１６】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末を使用しているユーザの識別情報であってもよい。

【００１７】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のホスト名であってもよい。

【００１８】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のＩＰアドレスであってもよい。

【００１９】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のＭＡＣアドレスであってもよい。

【００２０】また、本発明のネットワーク管理装置は、ネットワーク中継機器から端末の情報を受信した場合、前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信する機能を備えたものである。

【００２１】前記ネットワーク中継機器に返信するべきアクセス許可／禁止を示す情報と前記端末情報との対応を管理できる機能を備えてもよい。

【００２２】前記端末情報は、当該端末を使用しているユーザの識別情報であってもよい。

【００２３】前記端末情報は、当該端末のホスト名であってもよい。

【００２４】前記端末情報は、当該端末のＩＰアドレスであってもよい。

【００２５】前記端末情報は、当該端末のＭＡＣアドレスであってもよい。

【００２６】ＩＰアドレスと有効ビットマスク値とを組として複数のＩＰアドレスを指定するＩＰサブネットを用い、このＩＰサブネットとアクセス許可／禁止情報との対応を定義しておき、この定義に照らして前記アクセス許可／禁止情報と前記端末のＩＰアドレスとの対応を

管理する機能を備えてもよい。

【００２７】前記ネットワーク中継機器からの送信及びその送信に対する返信の内容をログとして記録し、このログを管理画面から参照できる機能を備えてもよい。

【００２８】

【発明の実施の形態】以下、本発明の実施形態を添付図面に基づいて詳述する。

【００２９】１）第一の実施形態

図１に示されるように、本発明に係るネットワーク管理システムは、本発明に係る２台のネットワーク中継機器１０１，１０２と、本発明に係るネットワーク管理装置１０３とを有する。ネットワーク中継機器は、例えば、スイッチングハブである。

【００３０】図２に示されるように、スイッチングハブ２０１は、１番～５番ポート２０２～２０６、中継回路２０７、プロセッサ２０８、メモリ２０９等から構成されている。

【００３１】以下に、スイッチングハブ２０１等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【００３２】（１）管理者は、予めポート毎に、端末が接続された場合に、その端末の情報をネットワーク管理装置に送信するかどうかを設定しておく。端末情報を送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【００３３】（２）管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【００３４】（３）管理者は、端末情報の送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【００３５】（４）ネットワーク中継機器は、自動使用可否設定ポートに新たに端末が接続された場合など、端末情報を送信するべき際、自動使用可否設定ポートが受信したフレームからホスト名等の端末を識別するための識別キーを検出し、その識別キーを端末情報としてネットワーク管理装置に送信する。

【００３６】（５）ネットワーク中継機器は、端末情報の送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【００３７】（６）ネットワーク中継機器は、端末情報の送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【００３８】（７）ネットワーク中継機器は、ネットワーク管理装置に端末情報を送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあったとおりに使用可否の設定を行う。

【００３９】（８）以上によって設定された各設定内容（ネットワーク中継機器の構成情報と呼ぶ）はメモリ２０９に格納される。爾後、中継回路２０７は、ネットワーク中継機器２０１の構成情報を通信処理に使用する。

【００４０】以下に、ネットワーク管理装置１０３が行う処理を示す。

【００４１】（１）各端末とポートの使用可否との管理テーブル（ホスト名とアクセス許可／禁止情報とを対応させて登録したもの）１０４を内部に持っており、管理画面上からこの管理テーブルの設定ができる。

【００４２】（２）ネットワーク中継機器から端末情報である識別キー（ホスト名）が送信された場合、管理テーブル１０４から端末を検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【００４３】（３）ネットワーク中継機器からの問い合わせ（端末情報を送信すること）及びその問い合わせに対する返信の内容をログとして記録する。このログは、管理画面から参照できる。

【００４４】図１を用いて、より具体的な流れを説明する。ここでは、端末情報は端末のホスト名である。

【００４５】ネットワーク中継機器１０１の１番ポート～４番ポート及びネットワーク中継機器１０２の１番ポート、３番ポート～５番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器１０１の５番ポート及びネットワーク中継機器１０２の２番ポートは、自機及び接続される端末が上位ネットワークと通信できるように使用可能に設定されているものとする。

【００４６】また、ネットワーク中継機器１０１，１０２には、端末情報の送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置１０３のアドレスが設定されているものとする。

【００４７】ネットワーク管理装置１０３には、図示のように、予め内部の管理テーブル１０４に設定がなされているものとする。

【００４８】いま、ホスト名がｒｅｄの端末１０５がネットワーク中継機器１０１の１番ポートに接続されたとする。端末１０５からフレームが送信されると、ネットワーク中継機器１０１のフィルタリングテーブル（図示せず）にフレームから抽出した端末１０５のＭＡＣアドレスが登録される。そのタイミングでネットワーク中継機器１０１は、端末１０５のＩＰアドレスを検出し、ＤＮＳによりホスト名を検索し、そのホスト名をネットワーク管理装置１０３に送信する。

【００４９】ネットワーク管理装置１０３は、受信したホスト名に対応したデータを管理テーブル１０４から検索する。ホスト名ｒｅｄは、アクセスが許可と設定されているので、ネットワーク管理装置１０３は、アクセス許可を示す情報をネットワーク中継機器１０１に返信する。

【００５０】アクセス許可を示す情報を受信したネットワーク中継機器１０１は、端末１０５が接続されている

１番ポートを使用可能にする。これにより、端末１０５は、ネットワーク中継機器１０１を介してネットワークにアクセスすることができるようになる。

【００５１】同様に、ホスト名がｒｅｄの端末１０５がネットワーク中継機器１０２の３番ポートに接続された場合も、ネットワーク中継機器１０２の３番ポートは利用可能に設定される。つまり、この端末１０５は、どのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることになる。

【００５２】端末１０５のホスト名がｂｌｕｅの場合、管理テーブル１０４にアクセスが禁止と設定されているので、ネットワーク中継機器１０１，１０２からの問い合わせに対してネットワーク管理装置１０３からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器１０１，１０２は、端末１０５が接続されているポートを使用不可にする。これにより、端末１０５は、ネットワーク中継機器１０１，１０２を介してネットワークにアクセスすることができない。

【００５３】端末１０５のホスト名がｇｒａｙの場合、管理テーブル１０４に該当するホスト名が登録されていないため、管理テーブル１０４の“その他”のデータが参照され、そのデータにはアクセスが禁止と設定されているので、ネットワーク中継機器１０１，１０２からの問い合わせに対してネットワーク管理装置１０３からアクセス禁止を示す情報が返信される。ネットワーク中継機器１０１，１０２は、端末１０５が接続されているポートを使用不可にするので、端末１０５は、ネットワーク中継機器１０１，１０２を介してネットワークにアクセスすることができない。これにより、不明なホスト名が設定されている端末をネットワークにアクセスさせることを防ぐことができる。

【００５４】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置１０３に記録され、後に管理者がそのログを管理画面から参照することができる。

【００５５】ネットワーク中継機器１０１，１０２とネットワーク管理装置１０３との通信ができなかった場合など、端末情報の送信に対する返信がなかった場合、ネットワーク中継機器１０１，１０２は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【００５６】このようにして設定されたネットワーク中継機器の構成情報は、メモリ２０９に格納され、中継回路２０７によって通信処理に使用される。

【００５７】２）第二の実施形態

図３に示されるように、本発明に係るネットワーク管理システムは、本発明に係る２台のネットワーク中継機器１０１，１０２と、本発明に係るネットワーク管理装置１０３とを有する。ネットワーク中継機器は、例えば、スイッチングハブであり、図２に示した内部構成を有する。

【００５８】以下に、スイッチングハブ２０１等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【００５９】（１）管理者は、予めポート毎に、そのポートで受信したデータの内容から端末使用者のユーザＩＤ（識別情報）を検知した場合にそのユーザＩＤを端末情報としてネットワーク管理装置に送信するかどうかを設定しておく。検知したユーザＩＤを送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【００６０】（２）管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【００６１】（３）管理者は、ユーザＩＤの送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【００６２】（４）ネットワーク中継機器は、あるポートで受信したデータの内容から端末使用者のユーザＩＤを検知した場合、そのユーザＩＤを端末情報としてネットワーク管理装置に送信する。

【００６３】（５）ネットワーク中継機器は、ユーザＩＤの送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【００６４】（６）ネットワーク中継機器は、ユーザＩＤの送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【００６５】（７）ネットワーク中継機器は、ネットワーク管理装置にユーザＩＤを送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあった通りに使用可否の設定を行う。

【００６６】（８）以上によって設定されたネットワーク中継機器の構成情報はメモリ２０９に格納される。爾後、中継回路２０７は、ネットワーク中継機器の構成情報を通信処理に使用する。

【００６７】以下に、ネットワーク管理装置１０３が行う処理を示す。

【００６８】（１）各ユーザＩＤとポートの使用可否との管理テーブル（ユーザＩＤとアクセス許可／禁止情報とを対応させて登録したもの）１０４を内部に持っており、管理画面上からこの管理テーブル１０４の設定ができる。

【００６９】（２）ネットワーク中継機器から端末情報であるユーザＩＤが送信された場合、管理テーブル１０４から端末を検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【００７０】（３）ネットワーク中継機器からの問い合わせ及びその問い合わせに対する返信の内容をログとし

て記録する。このログは、管理画面から参照できる。

【００７１】図３を用いて、より具体的な流れを説明する。

【００７２】ネットワーク中継機器１０１の１番ポート～４番ポート及びネットワーク中継機器１０２の１番ポート、３番ポート～５番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器１０１の５番ポート及びネットワーク中継機器１０２の２番ポートは、自機及び接続される端末が上位ネットワークと通信できるように使用可能に設定されているものとする。

【００７３】また、ネットワーク中継機器１０１，１０２には、ユーザＩＤの送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置１０３のアドレスが設定されているものとする。

【００７４】ネットワーク管理装置１０３には、図示のように、予め内部の管理テーブル１０４に設定がなされているものとする。

【００７５】いま、端末１０５がネットワーク中継機器１０１の１番ポートに接続されていたとする。ログイン名“Ｙａｍａｍｏｔｏ”のユーザＩＤを持つユーザが端末１０５にログインすると、端末１０５からログイン情報を持つフレームが送信されるので、ネットワーク中継機器１０１は、そのフレームからユーザＩＤ“Ｙａｍａｍｏｔｏ”を検出し、このユーザＩＤをネットワーク管理装置１０３に送信する。

【００７６】ネットワーク管理装置１０３は、受信したユーザＩＤに対応したデータを管理テーブル１０４から検索する。この例では、ユーザＩＤ“Ｙａｍａｍｏｔｏ”に対しアクセスが許可と設定されているので、ネットワーク管理装置１０３は、アクセス許可を示す情報をネットワーク中継機器１０１に返信する。

【００７７】アクセス許可を示す情報を受信したネットワーク中継機器１０１は、端末１０５が接続されている１番ポートを使用可能にする。これにより、端末１０５は、ネットワーク中継機器１０１を介してネットワークにアクセスすることができるようになる。

【００７８】同様に、端末１０５がネットワーク中継機器１０２の３番ポートに接続された場合も、“Ｙａｍａｍｏｔｏ”のユーザＩＤを持つユーザがログインすれば、ネットワーク中継機器１０２の３番ポートは利用可能に設定される。

【００７９】また、ネットワーク中継機器１０２の５番ポートに接続された別の端末１０６に“Ｙａｍａｍｏｔｏ”のユーザＩＤを持つユーザがログインした場合も、ネットワーク中継機器１０２の５番ポートは利用可能に設定される。つまり、ユーザＩＤ“Ｙａｍａｍｏｔｏ”を使用するユーザは、どの端末を使用しても、また端末をどのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることになる。

【００８０】端末１０５のユーザＩＤが“Ｋａｗａｇｕｔｉ”の場合、管理テーブル１０４にアクセスが禁止と設定されているので、ネットワーク中継機器１０１，１０２からの問い合わせに対してネットワーク管理装置１０３からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器１０１，１０２は、端末１０５が接続されているポートを使用不可にする。これにより、端末１０５は、ネットワーク中継機器１０１，１０２を介してネットワークにアクセスすることができない。

【００８１】端末１０５のユーザＩＤが“Ｙａｍａｄａ”の場合、管理テーブル１０４に該当するユーザＩＤが登録されていないため、管理テーブル１０４の“その他”のデータが参照され、そのデータにはアクセスが禁止と設定されているので、ネットワーク中継機器１０１，１０２からの問い合わせに対してネットワーク管理装置１０３からアクセス禁止を示す情報が返信される。ネットワーク中継機器１０１，１０２は、端末１０５が接続されているポートを使用不可にするので、端末１０５は、ネットワーク中継機器１０１，１０２を介してネットワークにアクセスすることができない。これにより、不明なユーザＩＤを使用してログインされる端末をネットワークにアクセスさせることを防ぐことができる。

【００８２】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置１０３に記録され、後に管理者がそのログを管理画面から参照することができる。

【００８３】ネットワーク中継機器１０１，１０２とネットワーク管理装置１０３との通信ができなかった場合など、端末情報の送信に対する返信がなかった場合、ネットワーク中継機器１０１，１０２は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【００８４】このようにして設定されたネットワーク中継機器の構成情報は、メモリ２０９に格納され、中継回路２０７によって通信処理に使用される。

【００８５】３）第三の実施形態

図４に示されるように、本発明に係るネットワーク管理システムは、本発明に係る２台のネットワーク中継機器１０１，１０２と、本発明に係るネットワーク管理装置１０３とを有する。ネットワーク中継機器は、例えば、スイッチングハブであり、図２に示した内部構成を有する。

【００８６】以下に、スイッチングハブ２０１等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【００８７】（１）管理者は、予めポート毎に、端末が接続された場合に、その端末のＩＰアドレスを端末情報

としてネットワーク管理装置に送信するかどうかを設定しておく。端末情報を送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【００８８】（２）管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【００８９】（３）管理者は、ＩＰアドレスの送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【００９０】（４）ネットワーク中継機器は、フィルタリングテーブル（図示せず）に新たにＭＡＣアドレスが登録される場合など、端末のＩＰアドレスを送信するべき際、自動使用可否設定ポートが受信したフレームから端末のＩＰアドレスを検出し、そのＩＰアドレスをネットワーク管理装置に送信する。

【００９１】（５）ネットワーク中継機器は、ＩＰアドレスの送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【００９２】（６）ネットワーク中継機器は、ＩＰアドレスの送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【００９３】（７）ネットワーク中継機器は、ネットワーク管理装置にＩＰアドレスを送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあったとおりに使用可否の設定を行う。

【００９４】（８）以上によって設定されたネットワーク中継機器の構成情報はメモリ２０９に格納される。爾後、中継回路２０７は、ネットワーク中継機器２０１の構成情報を通信処理に使用する。

【００９５】以下に、ネットワーク管理装置１０３が行う処理を示す。

【００９６】（１）各ＩＰアドレス（ＩＰサブネット含む）とポートの使用可否との管理テーブル（ＩＰアドレス又はＩＰサブネットとアクセス許可／禁止情報とを対応させて登録したもの）１０４を内部に持っており、管理画面上からこの管理テーブルの設定ができる。ここで、ＩＰサブネットは、ＩＰアドレスと有効ビットマスク値とを組とするものであり、このＩＰサブネットを用いて複数のＩＰアドレスを指定することができる。

【００９７】（２）ネットワーク中継機器からＩＰアドレスが送信された場合、管理テーブル１０４からＩＰアドレスを検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【００９８】（３）受信したＩＰアドレスと一致するＩＰアドレスが管理テーブル１０４に登録されていない場合、管理テーブル１０４に登録されているＩＰサブネットの中で、適合する最もサブネットマスク長が長いＩＰサブネットを検索し、このＩＰサブネットに対応するアクセス許可／禁止情報を前記ネットワーク中継機器に返信する。

【００９９】（４）ネットワーク中継機器からの問い合わせ及びその問い合わせに対する返信の内容をログとして記録する。このログは、管理画面から参照できる。

【０１００】図４を用いて、より具体的な流れを説明する。

【０１０１】ネットワーク中継機器１０１の１番ポート～４番ポート及びネットワーク中継機器１０２の１番ポート、３番ポート～５番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器１０１の５番ポート及びネットワーク中継機器１０２の２番ポートは、自機及び接続される端末が上位ネットワークと通信できるように使用可能に設定されているものとする。

【０１０２】また、ネットワーク中継機器１０１，１０２には、ＩＰアドレスの送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置１０３のアドレスが設定されているものとする。

【０１０３】ネットワーク管理装置１０３には、図示のように、予め内部の管理テーブル１０４に設定がなされているものとする。

【０１０４】いま、ＩＰアドレスが１７２．１７．３３．１の端末１０５がネットワーク中継機器１０１の１番ポートに接続されたとする。端末１０５からフレームが送信されると、ネットワーク中継機器１０１のフィルタリングテーブルにフレームから抽出した端末１０５のＭＡＣアドレスが登録される。そのタイミングでネットワーク中継機器１０１は、ＩＰアドレスを検出し、そのＩＰアドレスをネットワーク管理装置１０３に送信する。

【０１０５】ネットワーク管理装置１０３は、受信したＩＰアドレスに対応したデータを管理テーブル１０４から検索する。ＩＰアドレス１７２．１７．３３．１は、アクセスが許可と設定されているので、ネットワーク管理装置１０３は、アクセス許可を示す情報をネットワーク中継機器１０１に返信する。

【０１０６】アクセス許可を示す情報を受信したネットワーク中継機器１０１は、端末１０５が接続されている１番ポートを使用可能にする。これにより、端末１０５は、ネットワーク中継機器１０１を介してネットワークにアクセスすることができるようになる。

【０１０７】同様に、この端末１０５がネットワーク中継機器１０２の３番ポートに接続された場合も、ネットワーク中継機器１０２の３番ポートは利用可能に設定される。つまり、この端末１０５は、どのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることになる。

【０１０８】端末１０５のＩＰアドレスが１７２．１７．３３．２の場合、管理テーブル１０４にアクセスが

禁止と設定されているので、ネットワーク中継機器１０１，１０２からの問い合わせに対してネットワーク管理装置１０３からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器１０１，１０２は、端末１０５が接続されているポートを使用不可にする。これにより、端末１０５は、ネットワーク中継機器１０１，１０２を介してネットワークにアクセスすることができない。

【０１０９】端末１０５のＩＰアドレスが１７２．１７．３３．３の場合、管理テーブル１０４に一致するＩＰが登録されていない。この場合、適合するＩＰサブネットであって最もサブネットマスク長が長いＩＰサブネットのデータが使用される。従って、１７２．１７．３３．３については、１７２．１７．３３．＊／２４のＩＰサブネットがこの条件に適合するので、対応するアクセス許可を示す情報が返信される。

【０１１０】同様に、端末１０５のＩＰアドレスが１７１．１．１．１．の場合は、ＩＰサブネット１７１．＊．＊．＊／８が適合し、アクセス許可を示す情報が返信される。端末１０５のＩＰアドレスが１７０．１．１．１の場合は、ＩＰサブネット＊．＊．＊．＊／０が適合し、アクセス禁止を示す情報が返信される。

【０１１１】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置１０３に記録され、後に管理者がそのログを管理画面から参照することができる。

【０１１２】ネットワーク中継機器１０１，１０２とネットワーク管理装置１０３との通信ができなかった場合など、ＩＰアドレスの送信に対する返信がなかった場合、ネットワーク中継機器１０１，１０２は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【０１１３】このようにして設定されたネットワーク中継機器の構成情報は、メモリ２０９に格納され、中継回路２０７によって通信処理に使用される。

【０１１４】４）第四の実施形態

図５に示されるように、本発明に係るネットワーク管理システムは、本発明に係る２台のネットワーク中継機器１０１，１０２と、本発明に係るネットワーク管理装置１０３とを有する。ネットワーク中継機器は、例えば、スイッチングハブであり、図２に示した内部構成を有する。

【０１１５】以下に、スイッチングハブ２０１等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【０１１６】（１）管理者は、予めポート毎に、端末が接続された場合に、その端末のＭＡＣアドレスを端末情報としてネットワーク管理装置に送信するかどうかを設定しておく。端末情報を送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【０１１７】（２）管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【０１１８】（３）管理者は、ＭＡＣアドレスの送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【０１１９】（４）ネットワーク中継機器は、フィルタリングテーブル（図示せず）に新たにＭＡＣアドレスが登録される場合など、端末のＭＡＣアドレスを送信するべき際、自動使用可否設定ポートが受信したフレームから端末のＭＡＣアドレスを検出し、そのＭＡＣアドレスをネットワーク管理装置に送信する。

【０１２０】（５）ネットワーク中継機器は、ＭＡＣアドレスの送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【０１２１】（６）ネットワーク中継機器は、ＭＡＣアドレスの送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【０１２２】（７）ネットワーク中継機器は、ネットワーク管理装置にＭＡＣアドレスを送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあったとおりに使用可否の設定を行う。

【０１２３】（８）以上によって設定されたネットワーク中継機器の構成情報はメモリ２０９に格納される。爾後、中継回路２０７は、ネットワーク中継機器２０１の構成情報を通信処理に使用する。

【０１２４】以下に、ネットワーク管理装置１０３が行う処理を示す。

【０１２５】（１）各ＭＡＣアドレスとポートの使用可否との管理テーブル（ＭＡＣアドレスとアクセス許可／禁止情報とを対応させて登録したもの）１０４を内部に持っており、管理画面上からこの管理テーブルの設定ができる。

【０１２６】（２）ネットワーク中継機器からＭＡＣアドレスが送信された場合、管理テーブル１０４からＭＡＣアドレスを検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【０１２７】（３）ネットワーク中継機器からの問い合わせ及びその問い合わせに対する返信の内容をログとして記録する。このログは、管理画面から参照できる。

【０１２８】図５を用いて、より具体的な流れを説明する。

【０１２９】ネットワーク中継機器１０１の１番ポート～４番ポート及びネットワーク中継機器１０２の１番ポート、３番ポート～５番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器１０１の５番ポート及びネットワーク中継機器１０２の２番ポートは、自機及び接続される端末が上位ネット

ワークと通信できるように使用可能に設定されているものとする。

【０１３０】また、ネットワーク中継機器１０１，１０２には、ＭＡＣアドレスの送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置１０３のアドレスが設定されているものとする。

【０１３１】ネットワーク管理装置１０３には、図示のように、予め内部の管理テーブル１０４に設定がなされているものとする。

【０１３２】いま、ＭＡＣアドレスが１１：１１：１１：１１：１１：１１の端末１０５がネットワーク中継機器１０１の１番ポートに接続されたとする。端末１０５からフレームが送信されると、ネットワーク中継機器１０１のフィルタリングテーブルにフレームから抽出した端末１０５のＭＡＣアドレスが登録される。そのタイミングでネットワーク中継機器１０１は、そのＭＡＣアドレスをネットワーク管理装置１０３に送信する。

【０１３３】ネットワーク管理装置１０３は、受信したＭＡＣアドレスに対応したデータを管理テーブル１０４から検索する。ＭＡＣアドレス１１：１１：１１：１１：１１：１１は、アクセスが許可と設定されているので、ネットワーク管理装置１０３は、アクセス許可を示す情報をネットワーク中継機器１０１に返信する。

【０１３４】アクセス許可を示す情報を受信したネットワーク中継機器１０１は、端末１０５が接続されている１番ポートを使用可能にする。これにより、端末１０５は、ネットワーク中継機器１０１を介してネットワークにアクセスすることができるようになる。

【０１３５】同様に、この端末１０５がネットワーク中継機器１０２の３番ポートに接続された場合も、ネットワーク中継機器１０２の３番ポートは利用可能に設定される。つまり、この端末１０５は、どのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることになる。

【０１３６】端末１０５のＭＡＣアドレスが２２：２２：２２：２２：２２：２２の場合、管理テーブル１０４にアクセスが禁止と設定されているので、ネットワーク中継機器１０１，１０２からの問い合わせに対してネットワーク管理装置１０３からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器１０１，１０２は、端末１０５が接続されているポートを使用不可にする。これにより、端末１０５は、ネットワーク中継機器１０１，１０２を介してネットワークにアクセスすることができない。

【０１３７】端末１０５のＭＡＣアドレスが４４：４４：４４：４４：４４：４４の場合、管理テーブル１０４に該当するＭＡＣアドレスが登録されていないため、管理テーブル１０４の“その他”のデータが参照され、そのデータにはアクセスが禁止と設定されているので、ネットワーク中継機器１０１，１０２からの問い合わせに対してネットワーク管理装置１０３からアクセス禁止を示す情報が返信される。ネットワーク中継機器１０１，１０２は、端末１０５が接続されているポートを使用不可にするので、端末１０５は、ネットワーク中継機器１０１，１０２を介してネットワークにアクセスすることができない。これにより、不明なＭＡＣアドレスの端末をネットワークにアクセスさせることを防ぐことができる。

【０１３８】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置１０３に記録され、後に管理者がそのログを管理画面から参照することができる。

【０１３９】ネットワーク中継機器１０１，１０２とネットワーク管理装置１０３との通信ができなかった場合など、ＭＡＣアドレスの送信に対する返信がなかった場合、ネットワーク中継機器１０１，１０２は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【０１４０】このようにして設定されたネットワーク中継機器の構成情報は、メモリ２０９に格納され、中継回路２０７によって通信処理に使用される。

【０１４１】

【発明の効果】本発明は次の如き優れた効果を発揮する。

【０１４２】（１）ホスト名（識別キー）、ユーザＩＤ、ＩＰアドレス、ＭＡＣアドレス等の端末情報によって認証されている端末のみがネットワークにアクセスできるようになり、ネットワークのセキュリティを確保することができる。

【０１４３】（２）各端末毎或いは端末を利用するユーザ毎にポートの利用可否を統合管理することができる。

【０１４４】（３）ポート毎の接続端末の情報や利用可否設定のログを参照することができる。

【０１４５】（４）利用可否を管理するネットワーク管理装置のアドレスを自由に設定することができる。

【０１４６】（５）本発明によるポートの利用可否の設定を全ポートで使用しないこともできる。

【０１４７】（６）本発明によるポートの利用可否の設定をポート毎に使用するか否かを設定できる。

【０１４８】（７）端末情報の送信に対するネットワーク管理装置からの返信がなかった場合に端末が接続されているポートの使用可否をどうするかを予め指定しておくことができる。

【図面の簡単な説明】

【図１】本発明の第一の実施形態を示すネットワーク管理システムの構成図である。

【図２】本発明のネットワーク中継機器の実施形態を示すスイッチングハブの内部構成図である。

【図３】本発明の第二の実施形態を示すネットワーク管理システムの構成図である。

17

【図４】本発明の第三の実施形態を示すネットワーク管理システムの構成図である。

【図５】本発明の第四の実施形態を示すネットワーク管理システムの構成図である。

【符号の説明】

18

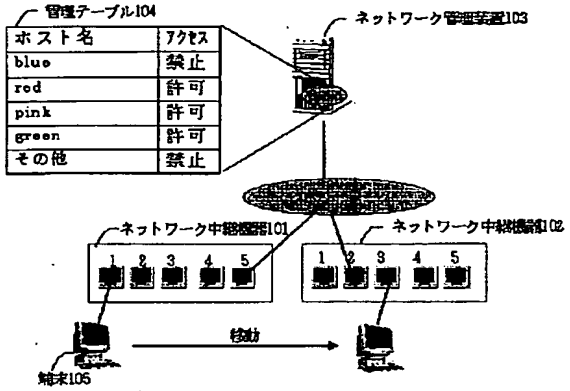
１０１，１０２　ネットワーク中継機器

１０３　ネットワーク管理装置

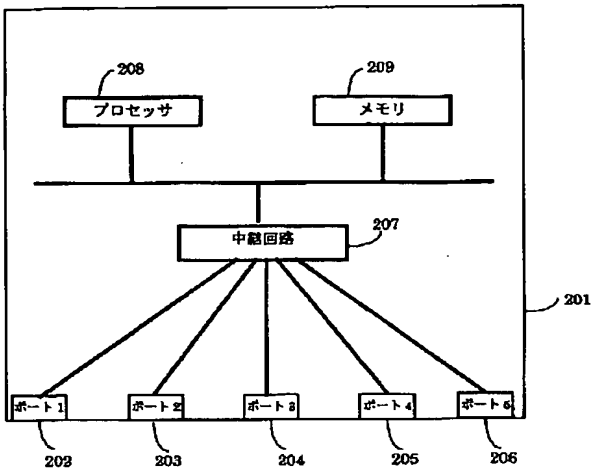
１０４　管理テーブル

１０５　端末

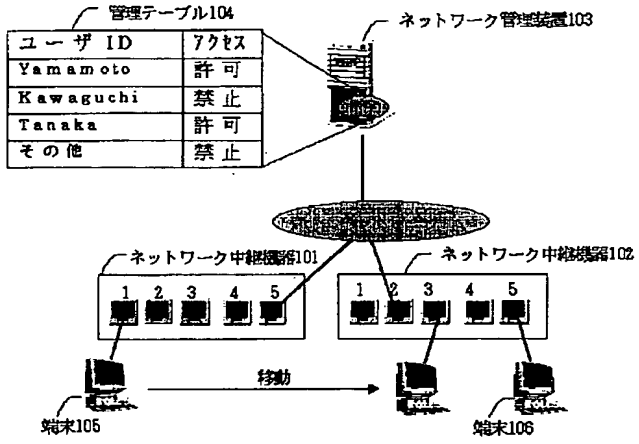
【図１】



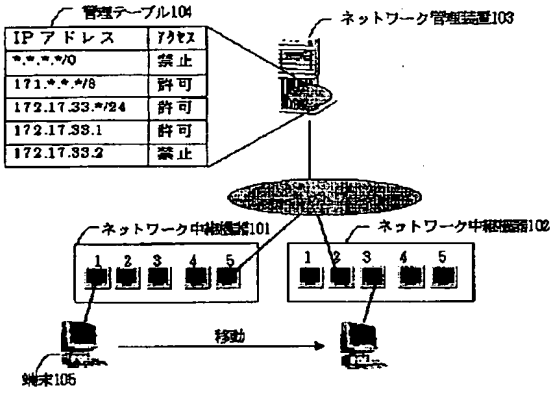
【図２】



【図３】



【図４】



【図５】